

JP2005109861

Publication Title:

ENCRYPTING DEVICE OF TRANSPORT STREAM, AND EDITING DEVICE,
AND METHODS FOR THEM

Abstract:

Abstract of JP2005109861

PROBLEM TO BE SOLVED: To edit contents with the copyright of the contents protected.

SOLUTION: An encrypting device is provided with a detecting means for detecting a TS (transport stream) header of an unencrypted transport stream, PES (packetized elementary stream) header, sequence header, GOP (group of picture) header and sequence end code, and an encrypting means for encrypting a transport stream excluding the TS header, PES header, sequence header, GOP header, and sequence end code. An editing device is provided with: a detecting means for detecting the TS header of a transport stream, PES header, sequence header, GOP header and sequence end code; and an editing means for editing an encrypted transport stream among TS packets having one and the same PID with a TS packet from which the GOP header is detected to a TS packet preceding a TS packet with the next GOP header detected as a unit without decrypting the encrypted transport stream.

COPYRIGHT: (C)2005,JPO&NCIP

Data supplied from the esp@cenet database - Worldwide and

Courtesy of <http://v3.espacenet.com>

(18) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2005-109861

(P2005-109861A)

(43) 公開日 平成17年4月21日(2005.4.21)

(51) Int. Cl. ⁷	F I	テーマコード (参考)
H04N 7/167	H04N 7/167	Z 5C053
H04L 9/36	H04N 5/91	N 5C064
H04N 5/91	H04N 5/82	H 5J104
H04N 5/92	H04L 9/00	685

審査請求 有 請求項の数 19 O L (全 14 頁)

(21) 出願番号	特願2003-340338 (P2003-340338)	(71) 出願人	000004237 日本電気株式会社 東京都港区芝五丁目7番1号
(22) 出願日	平成15年9月30日(2003.9.30)	(74) 代理人	100065385 弁理士 山下 穰平
		(74) 代理人	100122921 弁理士 志村 博
		(74) 代理人	100130029 弁理士 永井 道雄
		(74) 代理人	100065385 弁理士 山下 穰平
		(72) 発明者	沼井 祐一 東京都港区芝五丁目7番1号 日本電気株式会社内

最終頁に続く

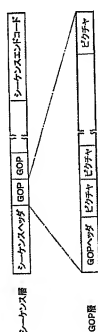
(54) 【発明の名称】 トランスポートストリームの暗号化装置及び編集装置並びにこれらの方法

(57) 【要約】

【課題】 コンテンツの著作権を保護したまま、コンテンツの編集をする。

【解決手段】 暗号化装置は、非暗号化トランスポートストリームのTSヘッダ、PESヘッダ、シーケンスヘッダ、GOPヘッダ及びシーケンスエンドコードを検出する検出手段と、TSヘッダ、PESヘッダ、シーケンスヘッダ、GOPヘッダ及びシーケンスエンドコードを除いてトランスポートストリームを暗号化する暗号化手段を備える。編集装置は、トランスポートストリームのTSヘッダ、PESヘッダ、シーケンスヘッダ、GOPヘッダ及びシーケンスエンドコードを検出する検出手段と、同一のPIDを有するTSパケットのうち、GOPヘッダが検出されたTSパケットから次のGOPヘッダが検出されたTSパケットまでのパケットを単位として、暗号化されたトランスポートストリームを暗号解読せずに編集する編集手段を備える。

【選択図】 図4



【特許請求の範囲】

【請求項1】

入力ストリームから編集単位のヘッダ及び前記ヘッダを検出するために必要な部分を少なくとも検出する検出手段と、

前記ヘッダ及び前記ヘッダを検出するための部分を少なくとも除いて前記入力ストリームを暗号化する暗号化手段と、

を備えることを特徴とするストリームの暗号化装置。

【請求項2】

請求項1に記載のストリーム暗号化装置により暗号化されたストリームから前記ヘッダを検出するために必要な部分及び前記ヘッダを検出する検出手段と、

前記編集単位で前記ストリームを暗号化されたままの状態に編集する編集手段と、

を備えることを特徴とするストリームの編集装置。

【請求項3】

暗号化されていないトランスポートストリームのTSヘッダ、TSパケットのペイロードに在るPESパケットのPESヘッダ及びビデオPESパケットのペイロードに在るGOPヘッダを少なくとも検出する検出手段と、

検出された前記TSヘッダ、前記PESヘッダ及び前記GOPヘッダを少なくとも除いて前記トランスポートストリームを暗号化する暗号化手段と、

を備えることを特徴とするトランスポートストリームの暗号化装置。

【請求項4】

請求項3に記載のトランスポートストリームの暗号化装置において、

前記検出手段は、前記ビデオPESパケットのペイロードに在るシーケンスヘッダ及びシーケンスエンドコードも検出し、

前記暗号化手段は、検出された前記シーケンスヘッダ及び前記シーケンスエンドコードも除いて前記トランスポートストリームを暗号化することを特徴とするトランスポートストリームの暗号化装置。

【請求項5】

請求項3に記載の暗号化装置において、

前記暗号化手段は、異なるGOPを含むTSパケットを異なる暗号鍵で暗号化することを特徴とするトランスポートストリームの暗号化装置。

【請求項6】

請求項3に記載の暗号化装置において、

前記暗号化されていないトランスポートストリーム又は前記暗号化されたトランスポートストリームから動画像を復元する動画像復元手段と、

前記復元された動画像を基に全部又は一部のGOPのそれぞれに対応した代表画像を生成する代表画像生成手段と、

を更に備えることを特徴とするトランスポートストリームの暗号化装置。

【請求項7】

請求項3に記載のトランスポートストリームの暗号化装置により暗号化されたトランスポートストリームのTSヘッダ、TSパケットのペイロードに在るPESパケットのPESヘッダ及びビデオPESパケットのペイロードに在るGOPヘッダを検出する検出手段と、

同一のPIDを有するTSパケットのうち、GOPヘッダが検出されたTSパケットから次のGOPヘッダが検出されたTSパケットの前のTSパケットまでを単位として、前記暗号化されたトランスポートストリームを暗号解読せずに編集する編集手段と、

を備えることを特徴とするトランスポートストリームの編集装置。

【請求項8】

請求項3に記載のトランスポートストリームの暗号化装置により暗号化されたトランスポートストリームのTSヘッダ、TSパケットのペイロードに在るPESパケットのPES

Sヘッダ及びビデオPESパケットのペイロードに在るGOPヘッダを検出する検出手段と、

同一のPIDを有するTSパケットのうち、GOPヘッダが検出されたTSパケットから次のGOPヘッダが検出されたTSパケットの前のTSパケットまでを単位として、前記代表画像を参照してユーザにより選択されたGOPが含まれるように、前記暗号化されたトランスポートストリームを暗号解読せずに編集する編集手段と、

を備えることを特徴とするトランスポートストリームの編集装置。

【請求項9】

請求項7又は8に記載のトランスポートストリームの編集装置において、

前記検出手段は、前記ビデオPESパケットのペイロードにあるシーケンスヘッダ及びシーケンスエンドコードも検出することを特徴とするトランスポートストリームの編集装置。

【請求項10】

入力ストリームから編集単位のヘッダ及び前記ヘッダを検出するために必要な部分を少なくとも検出する検出ステップと、

前記ヘッダ及び前記ヘッダを検出するための部分を少なくとも除いて前記入力ストリームを暗号化する暗号化ステップと、

を備えることを特徴とするストリームの暗号化方法。

【請求項11】

請求項10に記載のストリーム暗号化方法により暗号化されたストリームから前記ヘッダを検出するために必要な部分及び前記ヘッダを検出する検出ステップと、

前記編集単位で前記ストリームを暗号化されたままの状態編集する編集ステップと、

を備えることを特徴とするストリームの編集方法。

【請求項12】

暗号化されていないトランスポートストリームのTSヘッダ、TSパケットのペイロードに在るPESパケットのPESヘッダ及びビデオPESパケットのペイロードに在るGOPヘッダを少なくとも検出する検出ステップと、

検出された前記TSヘッダ、前記PESヘッダ及び前記GOPヘッダを少なくとも除いて前記トランスポートストリームを暗号化する暗号化ステップと、

を備えることを特徴とするトランスポートストリームの暗号化方法。

【請求項13】

請求項12に記載のトランスポートストリームの暗号化方法において、

前記検出ステップは、前記ビデオPESパケットのペイロードに在るシーケンスヘッダ及びシーケンスエンドコードも検出し、

前記暗号化ステップは、検出された前記シーケンスヘッダ及び前記シーケンスエンドコードも除いて前記トランスポートストリームを暗号化することを特徴とするトランスポートストリームの暗号化方法。

【請求項14】

請求項12に記載の暗号化方法において、

前記暗号化ステップは、異なったGOPを含むTSパケットを異なった暗号鍵で暗号化することを特徴とするトランスポートストリームの暗号化方法。

【請求項15】

請求項12に記載の暗号化方法において、

前記暗号化されていないトランスポートストリーム又は前記暗号化されたトランスポートストリームから動画像を復元する動画像復元ステップと、

前記復元された動画像を基に全部又は一部のGOPのそれぞれに対応した代表画像を生成する代表画像生成ステップと、

を更に備えることを特徴とするトランスポートストリームの暗号化方法。

【請求項16】

請求項12に記載のトランスポートストリームの暗号化方法により暗号化されたトラン

スポーツストリームのTSヘッダ、TSパケットのペイロードに在るPESパケットのPESヘッダ及びビデオPESパケットのペイロードに在るGOPヘッダを検出する検出ステップと、

同一のPIDを有するTSパケットのうち、GOPヘッダが検出されたTSパケットから次のGOPヘッダが検出されたTSパケットの前のTSパケットまでを単位として、前記暗号化されたトランスポートストリームを暗号解読せずに編集する編集ステップと、

を備えることを特徴とするトランスポートストリームの編集方法。

【請求項17】

請求項12に記載のトランスポートストリームの暗号化方法により暗号化されたトランスポートストリームのTSヘッダ、TSパケットのペイロードに在るPESパケットのPESヘッダ及びビデオPESパケットのペイロードに在るGOPヘッダを検出する検出ステップと、

同一のPIDを有するTSパケットのうち、GOPヘッダが検出されたTSパケットから次のGOPヘッダが検出されたTSパケットの前のTSパケットまでを単位として、前記代表画面像を参照してユーザにより選択されたGOPが含まれるように、前記暗号化されたトランスポートストリームを暗号解読せずに編集する編集ステップと、

を備えることを特徴とするトランスポートストリームの編集方法。

【請求項18】

請求項16又は17に記載のトランスポートストリームの編集方法において、

前記検出ステップは、前記ビデオPESパケットのペイロードにあるシーケンスヘッダ及びシーケンスエンドコードも検出することを特徴とするトランスポートストリームの編集方法。

【請求項19】

コンピュータに請求項10乃至18のいずれか1項に記載の方法を行わせるためのプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、MPEG(Moving Picture Experts Group)信号を含むトランスポートストリームの暗号化装置及び編集装置並びにこれらの方法に関する。

【背景技術】

【0002】

近年、デジタル信号処理技術の進歩に伴い、映像信号は、デジタル信号の形態で伝送及び蓄積がされるようになってきている。デジタル信号の伝送及び蓄積の方式としては、MPEG方式が標準化されている。

【0003】

図1に、パーソナルコンピュータをベースとしたMPEG信号の処理システムの従来例を示す。

【0004】

図1を参照すると、このシステムは、CPU901、ハードディスクドライブ902、デジタル放送処理ボード903、汎用バス904及び表示部905を備える。

【0005】

CPU901は、プログラムに従って、各種演算処理を行う。ハードディスクドライブ902は、各種プログラムやデータを格納し、特に、暗号化されたトランスポートストリームを格納する。デジタル放送処理ボード903は、デジタル放送より受信したトランスポートストリームの各種処理を行う。汎用バス904は、CPU901、ハードディスクドライブ902及びデジタル放送処理ボード903に接続され、これらの間で入出力するデータを運ぶ。表示部905は、各種画面を表示し、特にデジタル放送処理ボード903から出力された映像信号を入力し、その映像信号に従って映像を表示する。

【0006】

デジタル放送処理ボード903は、受信部911、暗号化部912、暗号解読部913

及びMPEGデコーダ914を備える。

【0007】

受信部911は、放送よりトランスポートストリームを受信する。暗号化部912は、受信部911が受信したトランスポートストリームを暗号化して、暗号化されたトランスポートストリームを汎用バス904に出力する。ハードディスクドライブ902はこの暗号化されたトランスポートストリームを格納する。ハードディスクドライブ902は、格納されている暗号化されたトランスポートストリームを出力する。暗号解読部913は、この暗号化されたトランスポートストリームの暗号解読を行い、暗号解読されたトランスポートストリームから映像部分を多重分離したMPEGビットストリームをMPEGデコーダ914に出力する。

【0008】

MPEGデコーダ914は、MPEGビットストリームを復号して、これにより得た映像信号を表示部905に出力する。

【0009】

このような構成によれば、汎用バス904に現れるトランスポートストリームは暗号化されているので、汎用バス904に現れたトランスポートストリームを不正にコピーすることができない。また、MPEGデコーダ914から出力された映像信号は直接表示部905に出力されるので、傍受することができない。このようにしてコンテンツの著作権を保護することができる。

【0010】

なお、本発明に関連する先行技術文献として、以下のものがある。

【特許文献1】特開平08-322034号公報

【特許文献2】特開平10-336624号公報

【特許文献3】特開2002-287624号公報

【特許文献4】特開2002-287625号公報

【特許文献5】特開2002-290999号公報

【発明の開示】

【発明が解決しようとする課題】

【0011】

しかしながら、図1に示すようなシステムを用いた場合、トランスポートストリームが暗号化部912により完全に暗号化されてしまうので、暗号解読部913により暗号解読を行わない限り、トランスポートストリームのどの部分にどのような映像が入っているのかを知ることができない。従って、暗号解読部913により暗号解読を行わない限り、コンテンツの編集をすることができない。

【0012】

つまり、暗号解読部913によって暗号解読したトランスポートストリームを図1で破線で示す編集部906により編集することとすると、ハードディスクドライブ902から読み出されたデータは、暗号解読部913で暗号解読された後、編集部906で処理された後に、暗号化部912で暗号化され、ハードディスクドライブ902に再書き込みされるため、暗号解読されたトランスポートストリームが図1で破線矢印で示すように汎用バス904に現れることとなり、著作権を保護することができなくなってしまう。

【0013】

また、暗号化部912が暗号化する前のトランスポートストリームから各GOPの代表画像を得て、その代表画像を見ながら編集することも考えられるが、このGOPを編集後のトランスポートストリームに含めたいことを希望しても、そのGOPがトランスポートストリームのどこにあるのかが不明であり、それを明らかにするためには、結局は、暗号化されているトランスポートストリームを暗号解読しなければならず、著作権の保護を図ることができない。

【0014】

そこで、本発明は、コンテンツの著作権を保護したまま、コンテンツの編集をすること

を可能とするトランスポートストリームの暗号化装置及び編集装置並びにそれらの方法を提供することを目的とする。

【課題を解決するための手段】

【0015】

本発明の第1の観点によれば、入力ストリームから編集単位のヘッダ及び前記ヘッダを検出するために必要な部分を少なくとも検出する検出手段と、前記ヘッダ及び前記ヘッダを検出するための部分を少なくとも除いて前記入力ストリームを暗号化する暗号化手段と、を備えることを特徴とするストリームの暗号化装置が提供される。

【0016】

本発明の第2の観点によれば、本発明の第1の観点によるストリーム暗号化装置により暗号化されたストリームから前記ヘッダを検出するために必要な部分及び前記ヘッダを検出する検出手段と、前記編集単位で前記ストリームを暗号化されたままの状態編集する編集手段と、を備えることを特徴とするストリームの編集装置が提供される。

【0017】

本発明の第3の観点によれば、暗号化されていないトランスポートストリームのTSヘッダ、TSパケットのペイロードに在るPESパケットのPESヘッダ及びビデオPESパケットのペイロードに在るGOPヘッダを少なくとも検出する検出手段と、検出された前記TSヘッダ、前記PESヘッダ及び前記GOPヘッダを少なくとも除いて前記トランスポートストリームを暗号化する暗号化手段と、を備えることを特徴とするトランスポートストリームの暗号化装置が提供される。

【0018】

本発明の第3の観点によるトランスポートストリームの暗号化装置において、前記検出手段は、前記ビデオPESパケットのペイロードに在るシーケンスヘッダ及びシーケンスエンドコードも検出し、前記暗号化手段は、検出された前記シーケンスヘッダ及び前記シーケンスエンドコードも除いて前記トランスポートストリームを暗号化してもよい。上記の暗号化装置において、前記暗号化手段は、異なったGOPを含むTSパケットを異なった暗号鍵で暗号化してもよい。

【0019】

上記の暗号化装置は、前記暗号化されていないトランスポートストリーム又は前記暗号化されたトランスポートストリームから動画像を復元する動画像復元手段と、前記復元された動画像を基に全部又は一部のGOPのそれぞれに対応した代表画像を生成する代表画像生成手段と、を更に備えていてもよい。

【0020】

本発明の第4の観点によれば、本発明の第1の観点によるトランスポートストリームの暗号化装置により暗号化されたトランスポートストリームのTSヘッダ、TSパケットのペイロードに在るPESパケットのPESヘッダ及びビデオPESパケットのペイロードに在るGOPヘッダを検出する検出手段と、同一のPIDを有するTSパケットのうち、GOPヘッダが検出されたTSパケットから次のGOPヘッダが検出されたTSパケットの前のTSパケットまでを単位として、前記暗号化されたトランスポートストリームを暗号化せずに編集する編集手段と、を備えることを特徴とするトランスポートストリームの編集装置が提供される。

【0021】

本発明の第5の観点によれば、本発明の第1の観点によるトランスポートストリームの暗号化装置により暗号化されたトランスポートストリームのTSヘッダ、TSパケットのペイロードに在るPESパケットのPESヘッダ及びビデオPESパケットのペイロードに在るGOPヘッダを検出する検出手段と、同一のPIDを有するTSパケットのうち、GOPヘッダが検出されたTSパケットから次のGOPヘッダが検出されたTSパケットの前のTSパケットまでを単位として、前記代表画像を参照してユーザにより選択されたGOPが含まれるように、前記暗号化されたトランスポートストリームを暗号化せずに編集する編集手段と、を備えることを特徴とするトランスポートストリームの編集装置が

提供される。

【0022】

本発明の第4の観点又は第5の観点によるトランスポートストリームの編集装置において、前記検出手段は、前記ビデオPESパケットのペイロードにあるシーケンスヘッダ及びシーケンスエンドコードも検出してよい。

【発明の効果】

【0023】

請求項1及び2に記載の発明によれば、暗号化されたストリームを暗号解読されなくてもストリームを編集単位で編集することが可能となるので、コンテンツの著作権を保護することが可能となる。

【0024】

請求項3に記載の発明によれば、TSヘッダ、PESヘッダ並びにシーケンスヘッダ、GOPヘッダ及びシーケンスエンドコードを除いてトランスポートストリームが暗号化されるので、暗号解読されなくても、TSヘッダ、PESヘッダ及びGOPヘッダを検出することが可能となり、従って、コンテンツの著作権を保護した状態で、コンテンツの編集することが可能となる。

【0025】

請求項4に記載の発明によれば、異なるGOPを含むTSパケットを異なる暗号鍵で暗号化するので、コンテンツの著作権をより厚く保護することができる。

【0026】

請求項5に記載の発明によれば、動画像を復元し、復元された動画像を基に全部又は一部のGOPのそれぞれに対応した代表画像を生成するので、編集時のユーザインターフェースを容易にすることができる。

【0027】

請求項6に記載の発明によれば、暗号解読せずに編集を行うので、コンテンツの著作権を保護した状態で、コンテンツの編集をすることができ、代表画像を参照してユーザにより選択されたGOPが含まれるように編集を行うので、ユーザインターフェースを容易にすることができる。

【0028】

請求項7に記載の発明によれば、暗号解読せずに編集を行うので、コンテンツの著作権を保護した状態で、コンテンツの編集をすることができると共に、代表画像を参照してユーザにより選択されたGOPが含まれるように編集を行うので、ユーザインターフェースを容易にすることができる。

【発明を実施するための最良の形態】

【0029】

以下、図面を参照して本発明を実施するための最良の形態について説明する。

【0030】

図2は、トランスポートストリームのフォーマット図を示す。図2を参照すると、トランスポートストリームは、複数のTS(Transport Stream)パケットより構成される。各TSパケットは、固定長であり、TSヘッダとTSペイロードより構成される。後述するPES(Packetized Elementary Stream)は、一般に可変長であり、TSパケットより長い。従って、1つのPESパケットは分割され、複数のTSパケットのペイロードに跨って挿入される。新たなPESパケットが始まる時には、新たなTSパケットが用いられ、従って、PESヘッダは、必ずTSペイロードの先頭に在る。また、分割されたPESパケットのうち最後の分割されたPESパケットの長さがTSパケットのペイロードの長さよりも短い場合には、PESパケットの前にスタッフィングバイトが挿入され、TSパケットの長さが維持される。各PESパケットは、PESヘッダとPESペイロードより構成される。PESペイロードには、分断化されたエレメンタリーストリームが挿入される。特に、ビデオエレメンタリーストリームから作成されたPESパケットのことをビデオPESパケットという。

【0031】

図3は、GOP(Group Of Picture)及びビデオPESパケットのペイロードを示す。G

OPの先頭には、GOPヘッダが配置される。ビデオエレメンタリストリームをどのように分断してビデオPESパケットを作成するのは自由であるが、PESパケットの先頭がGOPの先頭と一致すると復号処理が容易となる。本実施形態では、図3に示すように、PESパケットの先頭がGOPの先頭と一致することとする。1つのPESパケットに含まれるピクチャ数は任意であるが、例えば、1つのPESパケットに1つのピクチャが含まれる。

【0032】

TSヘッダには、PID等が含まれる。同一のPESパケットから生成されたTSパケットのPIDは同一である。PESヘッダには、ストリームID、PESパケットレングス、PTS(presentation time stamp)、DTS(decoding time stamp)等が含まれる。1つのエレメンタリストリームは同一のストリームIDを持つPESパケットにより伝送される。そして、映像信号に対しては、0xE0～0xEFの範囲の値のストリームIDが割り当てられる。従って、TSヘッダに含まれるPID及びPESヘッダに含まれるストリームIDを調べるにより、どのTSパケットにどの系統の映像信号が含まれているのかを知ることができる。従って、TSヘッダに含まれるPID及びPESヘッダに含まれるストリームIDを調べるにより、着目している系統の映像信号のみを抜き出すことができる。

【0033】

GOPヘッダには、グループスタートコード、タイムコード(時、分、秒、ピクチャ)、クロズドGOP、ブローケンリンクが含まれる。

【0034】

編集は、GOPヘッダに含まれるタイムコードを基準として行われる。従って、編集を行うためには、GOPに含まれるタイムコードを検出しなければならない。トランスポートストリームからGOPヘッダを検出するためには、まず、トランスポートストリームからTSヘッダを検出することにより各TSパケットを認識し、認識されたTSパケットのペロードのうちの一部のものの先頭に挿入されているPESヘッダを検出することによりPESパケットを認識し、認識されたPESパケットのうちビデオPESをつなぎ合わせてビデオエレメンタリストリームを再構築し、再構築されたビデオエレメンタリストリームからGOPを再構成しなければならない。このような方法によりGOPヘッダを検出した場合には、どのTSパケットにGOPヘッダが含まれているのかを知ることができる。また上述したように、着目している系統の映像信号のみを抜き出すことができる。従って、着目している系統の映像信号のあるタイムコードからあるタイムコードまでの部分を含むTSパケットを抽出することができる。そして、抽出したTSパケットをつなぎ合わせ、その後、TSヘッダとPESパケットの間にオプションで挿入されているアダプテーションフィールドに含まれるPCR(Program Clock Reference)並びにPESヘッダに含まれているPTS及びDTSを調整することにより、編集を行うことができる。

【0035】

また、図4に示すように、1以上のGOP並びにシーケンスヘッダ及びシーケンスエンドコードはシーケンス層を構成する。シーケンスヘッダには、シーケンスヘッダコード、画面の縦横のサイズ、画面のアスペクト比、画像レート、ビットレート、VBVバッファサイズ及び量子化マトリックスが含まれる。そして、このようなシーケンスヘッダに含まれる情報は、編集後のTSストリームでそのまま引き継がなくてはならない。従って、GOP単位で編集をする場合であっても、シーケンス層を認識する必要がある。

【0036】

従って、本実施形態では、コンテンツが暗号化されたままの状態、編集をすることと可能とするために、TSヘッダ、PESヘッダ並びにシーケンスヘッダ、GOPヘッダ及びシーケンスエンドコードを暗号化せず、トランスポートストリームの他の部分のみを暗号化する。

【0037】

図5に、本発明の実施形態によるパーソナルコンピュータをベースとしたMPEG信号

の処理システムを示す。

【0038】

図5を参照すると、このシステムは、CPU101、ハードディスクドライブ102、デジタル放送処理ボード103、汎用バス104、表示部105及び編集部106を備える。

【0039】

CPU101は、プログラムに従って、各種演算処理を行う。ハードディスクドライブ102は、各種プログラムやデータを格納し、特に、暗号化されたトランスポートストリームを格納する。デジタル放送処理ボード103は、デジタル放送されてきたトランスポートストリームの各種処理を行う。汎用バス104は、CPU101、ハードディスクドライブ102、デジタル放送処理ボード103及び編集部106に接続され、これらの間で入出力するデータを運ぶ。表示部105は、各種画面を表示し、特にデジタル放送処理ボード103から入力した映像信号に従って映像を表示する。

【0040】

デジタル放送処理ボード103は、受信部111、暗号化部112、暗号解読部113、MPEGデコーダ114、検出部115及び代表画像生成部116を備える。

【0041】

受信部111は、放送よりトランスポートストリームを受信する。検出部115は、受信部111が受信したトランスポートストリームからTSヘッダ、PESヘッダ、シーケンスヘッダ並びにGOPヘッダ及びシーケンスエンドコードを検出する。暗号化部112は、受信部111が受信したトランスポートストリームのうちTSヘッダ、PESヘッダ並びにシーケンスヘッダ、GOPヘッダ及びシーケンスエンドコードを除く部分を暗号化して、一部が暗号化されたトランスポートストリームを汎用バス104に出力する。ハードディスクドライブ102は、この一部が暗号化されたトランスポートストリームを格納する。ハードディスクドライブ102は、格納されている一部が暗号化されたトランスポートストリームを出力し、暗号解読部113は、この一部が暗号化されたトランスポートストリームの暗号解読を行い、暗号解読されたトランスポートストリームから映像部分を多重分離したMPEGビットストリームをMPEGデコーダ114に出力する。MPEGデコーダ114は、MPEGビットストリームを復号して、これにより得た映像信号を表示部105に出力する。

【0042】

編集部106は、検出部106-1を備える。検出部115は、暗号化されていないトランスポートストリームからTSヘッダ、PESヘッダ並びにシーケンスヘッダ、GOPヘッダ及びシーケンスエンドコードを検出するのに対し、検出部106-1は、ハードディスクドライブ102に格納されている一部が暗号化されているトランスポートストリームからTSヘッダ、PESヘッダ並びにシーケンスヘッダ、GOPヘッダ及びシーケンスエンドコードを検出する。一部が暗号化されているトランスポートストリームのTSヘッダ、PESヘッダ並びにシーケンスヘッダ、GOPヘッダ及びシーケンスエンドコードは暗号化されていないので、検出部106-1は、検出部115と同様な方法により、ハードディスクドライブ102に格納されている一部が暗号化されているトランスポートストリームからTSヘッダ、PESヘッダ並びにシーケンスヘッダ、GOPヘッダ及びシーケンスエンドコードを検出することができる。そして、編集部106は、検出部106-1が検出したGOPに含まれているタイムコードを基準にして、一部が暗号化されているトランスポートストリームのうち必要なTSパケットのみを、暗号解読せずに寄せ集めて、新たな一部が暗号化されたトランスポートストリームを生成し、生成された一部が暗号化されたトランスポートストリームをハードディスクドライブ102に書き込む。従って、ハードディスクドライブ102と編集部106の間では、一部が暗号化されたトランスポートストリームがやり取りされることより、汎用バス104には暗号解読されたトランスポートストリームは現れず、コンテンツの著作権を保護することができる。

【0043】

編集部106は、タイムコードを基準として編集を行うが、これのみでは、ユーザインターフェースが取れない。そこで、代表画像生成部116を設けている。受信部111がトランスポートストリームを受信している時に、MPEGデコーダ114は、映像信号及びタイムコードを復元する。代表画像生成部116は、MPEGデコーダ114から復元映像信号及びタイムコードを入力し、全部又は一部(例えば、シーンチェンジ部)のGOPについて、復元映像信号から代表画像(例えば、GOPの最初のフレームのサムネイル)を作成し、その代表画像とタイムコードを関連付けて、ハードディスクドライブ102に書き込む。編集時には、編集部106は、代表画像を所定の方法により表示し、代表画像を用いて選択された範囲のタイムコードのGOPを寄せ集める。

【0044】

また、一旦、一部が暗号化されたトランスポートストリームがハードディスクドライブ102に格納された後に、ハードディスクドライブ102から一部が暗号化されたトランスポートストリームを読み出し、暗号解読部113で暗号解読し、MPEGデコーダ114で映像信号及びタイムコードを復元し、代表画像生成部116で代表画像を生成し、ハードディスクドライブ102に代表画像とタイムコードを関連付けて書き込んでよい。

【0045】

また、暗号化部112が暗号化を行う際、GOP毎に暗号鍵を変化させてもよい。

【0046】

具体的には、GOPのうちIピクチャを暗号化し、Iピクチャ以外のピクチャを暗号化しない。そして、Iピクチャ以外のピクチャにIピクチャの暗号解読するために必要な暗号鍵を電子透かし形態で埋め込んでおく。暗号解読の際には、まず、Iピクチャ以外のピクチャから電子透かしを検出し、検出された電子透かしから暗号鍵を抽出し、その暗号鍵を用いてIピクチャを暗号解読する。Iピクチャの暗号解読ができない限り、Iピクチャ以外のピクチャを復元することができないので、Iピクチャを暗号化するので、GOP全体を暗号化したのと同様な効果を得ることができる。

【0047】

又は、GOPのタイムコードとそのGOPを暗号解読するために必要な暗号鍵を対応付けたテーブルをデジタル放送処理ボード103の不揮発性メモリ(図示せず)に書き込んでおいて、再生時に、そのテーブルを用いてGOP毎に暗号解読を行うようにしてもよい。

【0048】

又は、GOPのタイムコードとデジタル放送処理ボード103の不揮発メモリに書き込んである一定倍数の暗号鍵のテーブルとの対応が取れる計算式に従い、そのGOPの暗号鍵としてもよい。さらに、デジタル放送処理ボード103の基本となる暗号鍵とGOPのタイムコードを元に計算式によってGOP毎の暗号鍵を生成してもよい。

【0049】

なお、受信部111、暗号化部112、暗号解読部113、MPEGデコーダ114、検出部115及び代表画像生成部116は、ハードウェアによって実現してもよいし、デジタル放送処理ボード103に搭載したCPUが、このCPUをこれらの部分として機能させるためのプログラムを実行することによって実現してもよい。また、編集部106及び検出部106-1は、ハードウェアによって実現してもよいし、CPU101が、このCPUをこれらの部分として機能させるためのプログラムを実行することによって実現してもよい。

【0050】

上記の説明では、トランスポートストリームを扱うこととしたが、上記と同様な考えの基にプログラムストリームを処理しても良い。すなわち、バックヘッダ、PESヘッダ、シーケンススタートコード、GOPヘッダ及びシーケンスエンドコードを除いてプログラムストリームを暗号化し、そのようなプログラムストリームからバックヘッダ、PESヘッダ、シーケンススタートコード、GOPヘッダ及びシーケンスエンドコードを検出し、暗号解読しないでGOP単位でプログラムストリームの編集を行う。

【産業上の利用可能性】

【0051】

本発明は、コンテンツの著作権を保護した状態で、コンテンツを編集することを利用することができる。

【図面の簡単な説明】

【0052】

【図1】従来例によるパーソナルコンピュータをベースとしたMPEG信号の処理システムの構成を示すブロック図である。

【図2】TSパケットのフォーマット図である。

【図3】GOPとPESパケットとの関係を示す図である。

【図4】シーケンス層とGOP層との関係を示す図である。

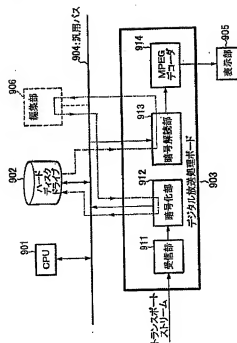
【図5】本発明の実施形態によるパーソナルコンピュータをベースとしたMPEG信号の処理システムの構成を示すブロック図である。

【符号の説明】

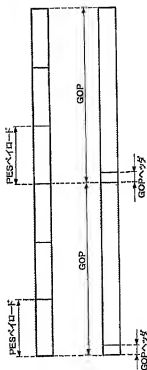
【0053】

- 101 CPU
- 102 ハードディスクドライブ
- 103 デジタル放送処理ボード
- 104 汎用バス
- 105 表示部
- 106 編集部
- 106-1 検出部
- 111 受信部
- 112 暗号化部
- 113 暗号解読部
- 114 MPEGデコーダ
- 115 検出部
- 116 代表画像生成部

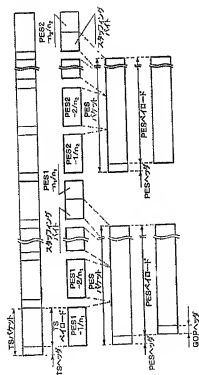
【図1】



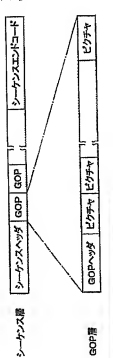
【図3】



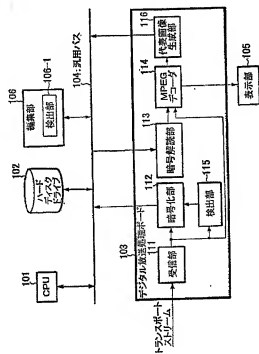
【図2】



【図4】



【図5】



Fターム(参考) 5C053 FA14 FA23 GA11 GB05 GB21 GB37 KA01 KA24 LA06 LA15

5C064 CA14

5J104 AA12

【要約の続き】